section, through security channels, only to DoD or other officials of the Federal Government who have an official need for such information.

§ 154.68 Safeguarding procedures.

Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

(a) Authorized requesters shall control and maintain accountability of all reports of investigation received.

(b) Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

(c) Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lockbar and an approved three-position dial-type combination padlock or in a similarly protected area/container.

(d) Reports of DoD personnel security investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows:

TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION

(e) An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in 32 CFR part 286.

§ 154.69 Records disposition.

(a) Personnel security investigative reports, to include OPM NACIs may be retained by DoD recipient organizations, only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with 32 CFR part 159.

(b) DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user—whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years.

(c) Personnel security investigative reports on persons who are considered for affiliation with DoD will be destroyed after 1 year if the affiliation is not completed.

§ 154.70 Foreign source information.

Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts. Further, information provided by foreign governments requesting an express promise of confidentiality shall be released only in a manner that will not identify or allow unauthorized persons to identify the foreign agency concerned.

Subpart K—Program Management

§ 154.75 General.

To ensure uniform implementation of the DoD personnel security program throughout the Department, program responsibility shall be centralized at DoD Component level.

§ 154.76 Responsibilities.

(a) The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security

program matters within the Department:

(1) Provide program management through issuance of policy and operating guidance.

(2) Provide staff assistance to the DoD Components and defense agencies in resolving day-to-day security policy and operating problems.

(3) Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

(4) Provide policy, oversight, and guidance to the component adjudication functions.

(5) Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

(b) The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD personnel security program management authorities.

(c) The Heads of the Components shall ensure that:

(1) The DoD personnel security program is administered within their area of responsibility in a manner consistent with this part.

(2) A single authority within the office of the head of the DoD Component is assigned responsibility for administering the program within the Component.

(3) Information and recommendations are provided the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)) and the General Counsel at their request concerning any aspect of the program.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

§ 154.77 Reporting requirements.

(a) The OASD(C31) shall be provided personnel security program management data by the Defense Data Manpower Center (DMDC) by December 31 each year for the preceding fiscal year. To facilitate accurate preparation of this report, all adjudicative determinations must be entered into the DC11 by all DoD central adjudication facilities no later than the end of the fiscal year. The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report shall cover the preceding fiscal year, broken out by clearance category, according to military (officer or enlisted), civilian or contractor status and by the central adjudication facility that took the action, using the enclosed format:

(1) Number of Top Secret, Secret, and Confidential clearances issued;

(2) Number of Top Secret, Secret, and Confidential clearances denied;

(3) Number of Top Secret, Secret, and Confidential clearances revoked;

(4) Number of SCI access determinations issued;

(5) Number of SCI access determinations denied;

(6) Number of SCI access determinations revoked; and

(7) Total number of personnel holding a clearance for Top Secret, Secret, Confidential and Sensitive Compartmented Information as of the end of the fiscal year.

(b) The Defense Investigative Service (DIS) shall provide the OASD(C3I) a quarterly report that reflects investigative cases opened and closed during the most recent quarter, by case category type, and by major requester. The information provided by DIS is essential for evaluating statistical data regarding investigative workload and the manpower required to perform personnel security investigations. Case category types include National Agency Checks (NACs); Expanded NACs; Single Scope Background Investigations (SSBIs), Periodic Reinvestigations (PRs); Secret Periodic Reinvestigations (SPRs); Post Adjudicative (PA); Special Investigative Inquiries (SIIs); and Limited Inquiries (LIs). This report shall be forwarded to OASD(C3I) within 45 days after the end of each quarter.